AR

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10303864 A

(43) Date of publication of application: 13.11.98

(51) Int. Cl H04K 1/02
H04N 1/44

(21) Application number: 09107793

(22) Date of filing: 24.04.97

(71) Applicant: FUJI XEROX CO LTD

(72) Inventor: KATSURABAYASHI MASAHIKO

(54) ENCIPHERMENT METHOD

(57) Abstract

PROBLEM TO BE SOLVED: To attain encipherment that is more difficult to decode by embedding the pseudo random numbers generated based on the initial data of a memory when the memory power supply is turned on into the blocks which are smaller than a prescribed size.

SOLUTION: The initial data stored in a prescribed address of a RAM are set as a variable a_0, and a pseudo random number a_1 is generated by a multiplication congruent method based on the number a_1. Then the numbers a_1 are continuously generated with the generated number a_1 defined as a new variable a_0. When an encipherment process is started, the generation of the number a_1 is stopped and at the same time the value of the variable a_0 is used as the initial value of the embedding data. When the data are enciphered in every block, the encipherment is repeated by DES in each block of 8 bytes. If the data to be processed are smaller than 8 bytes, the variable a_0 is used as the dummy embedding data. Then the data are enciphered by the DES when 8 bytes are secured. As a result, the data which are difficult to presume for the wiretappers can be embedded.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－303864

(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.⁶	識別記号	ＦＩ
Ｈ０４Ｋ　1/02		Ｈ０４Ｋ　1/02
Ｈ０４Ｎ　1/44		Ｈ０４Ｎ　1/44

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平9－107793

(22)出願日　平成９年(1997)４月24日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　桂林　正彦
埼玉県岩槻市府内３丁目７番１号　富士ゼロックス株式会社岩槻事業所内

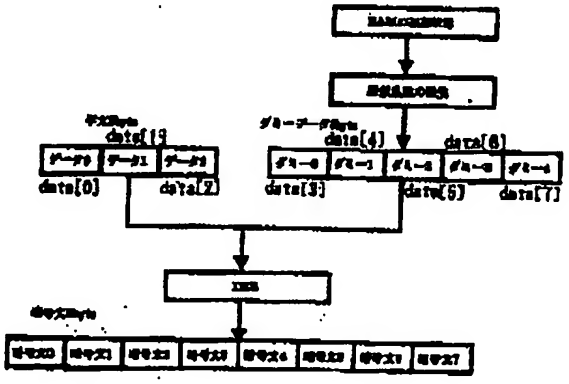
(74)代理人　弁理士　中島　淳　（外４名）

(54)【発明の名称】　暗号化方法

(57)【要約】

【課題】　データをブロック単位で暗号化する場合に、所定のブロックサイズに満たないブロックについては盗聴者に予想困難なデータを埋め込むことで、より解読困難な暗号化を行う。

【解決手段】　ＲＡＭの電源をオンした時に該ＲＡＭに記憶されていた初期データを記憶しておく。ブロック単位での暗号化処理において、最終ブロックが３バイトであった場合、ＲＡＭの初期データを基に発生させた擬似乱数を残りの５バイトのデータ（ｄａｔａ［３］～ｄａｔａ［７］）として埋め込む。そして、この擬似乱数を埋め込んだ最終ブロックをＤＥＳで暗号化する。



1

【特許請求の範囲】

【請求項１】 データをブロック単位で暗号化する暗号化方法であって、

メモリの電源をオンした時に該メモリに記憶されていた初期データを記憶しておき、

前記記憶した初期データを基に擬似乱数を発生させ、

データをブロック単位で暗号化する前に、前記発生させた擬似乱数を所定のブロックサイズに満たないブロックに埋め込む、

ことを特徴とする暗号化方法。

【請求項２】 データをブロック単位で暗号化する暗号化方法であって、

前の暗号化処理における平文を記憶しておき、

前記記憶した平文を基に擬似乱数を発生させ、

データをブロック単位で暗号化する前に、前記発生させた擬似乱数を所定のブロックサイズに満たないブロックに埋め込む、

ことを特徴とする暗号化方法。

【請求項３】 データをブロック単位で暗号化する暗号化方法であって、

暗号化処理の待機時に擬似乱数を連続的に発生させ、

データをブロック単位で暗号化する前に、当該時点で発生させた擬似乱数を所定のブロックサイズに満たないブロックに埋め込む、

ことを特徴とする暗号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、文字コードを含むデータを暗号化する暗号化方法に関する。

【０００２】

【従来の技術】通常の暗号化は所定ビット（ｎビット）のブロック単位で実行され、ｎビットの原データがｎビットの暗号化データに変換される。

【０００３】このようにｎビットのブロック単位で暗号化する暗号化方法において、原データのサイズがｎビットの倍数でない場合、ｎビットに満たない最終ブロックにランダムデータを埋め込んでｎビットとし、このランダムデータが埋め込まれた最終ブロックを暗号化することで、最終ブロックについての暗号強度を高める技術が特開平６－３２６８８０号公報に提案されている。

【０００４】ところが、特開平６－３２６８８０号公報では、具体的には日時データに基づいて作成されたランダムデータを最終ブロックに埋め込んでいる。これでは、暗号化した直後のファクシミリ送信時に盗聴された場合、盗聴者にとって暗号化した時刻は容易に予想できる。従って、最終ブロックに埋め込んだランダムデータも容易に予想できるので、最終ブロックについては盗聴者に予想され易い、という問題点があった。

【０００５】

【発明が解決しようとする課題】本発明は、上記問題点

2

を解消するために成されたものであり、データをブロック単位で暗号化する場合に、所定のブロックサイズに満たないブロックについては盗聴者に予想困難なデータを埋め込むことで、より解読困難な暗号化を行うことができる暗号化方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】上記目的を達成するために、請求項１記載の暗号化方法は、データをブロック単位で暗号化する暗号化方法であって、メモリの電源をオンした時に該メモリに記憶されていた初期データを記憶しておき、前記記憶した初期データを基に擬似乱数を発生させ、データをブロック単位で暗号化する前に、前記発生させた擬似乱数を所定のブロックサイズに満たないブロックに埋め込む、ことを特徴とする。

【０００７】また、請求項２記載の暗号化方法は、データをブロック単位で暗号化する暗号化方法であって、前の暗号化処理における平文を記憶しておき、前記記憶した平文を基に擬似乱数を発生させ、データをブロック単位で暗号化する前に、前記発生させた擬似乱数を所定のブロックサイズに満たないブロックに埋め込む、ことを特徴とする。

【０００８】また、請求項３記載の暗号化方法は、データをブロック単位で暗号化する暗号化方法であって、暗号化処理の待機時に擬似乱数を連続的に発生させ、データをブロック単位で暗号化する前に、当該時点で発生させた擬似乱数を所定のブロックサイズに満たないブロックに埋め込む、ことを特徴とする。

【０００９】上記請求項１記載の暗号化方法では、メモリの電源をオンした時に該メモリに記憶されていた初期データを記憶しておく。

【００１０】その後、暗号化処理を行う際に、前記記憶しておいた初期データを基に擬似乱数を発生させ、この擬似乱数を所定のブロックサイズに満たないブロックに埋め込む。そして、ブロック単位でのデータの暗号化を行う。

【００１１】このようにブロック単位でのデータの暗号化に先立ち、所定のブロックサイズに満たないブロックについては、盗聴者にとって予想困難なメモリの初期データに基づく擬似乱数を埋め込むので、より解読困難な暗号化を行うことができる。

【００１２】また、請求項２記載の暗号化方法では、前の暗号化処理における平文を記憶しておく。この平文は盗聴者にとって極めて予想困難である。

【００１３】その後、暗号化処理を行う際に、前記記憶しておいた平文を基に擬似乱数を発生させ、この擬似乱数を所定のブロックサイズに満たないブロックに埋め込む。そして、ブロック単位でのデータの暗号化を行う。

【００１４】このようにブロック単位でのデータの暗号化に先立ち、所定のブロックサイズに満たないブロックについては、盗聴者にとって予想困難な前処理の平文に

基づく擬似乱数を埋め込むので、より解読困難な暗号化を行うことができる。

【0015】また、請求項3記載の暗号化方法では、暗号化処理の待機時（暗号化処理を行っていない時）に擬似乱数を連続的に発生させる。その後、暗号化処理を行う際に、当該時点で発生させた擬似乱数を所定のブロックサイズに満たないブロックに埋め込み、ブロック単位でのデータの暗号化を行う。

【0016】暗号化処理の待機状態に関する情報（例えば、待機の開始時刻や待機時間の長さ等）は盗聴者にとって予想困難であるので、上記で埋め込んだ擬似乱数も盗聴者にとって予想困難である。このようにブロック単位でのデータの暗号化に先立ち、所定のブロックサイズに満たないブロックについては、盗聴者にとって予想困難な擬似乱数を埋め込むので、より解読困難な暗号化を行うことができる。

【0017】

【発明の実施の形態】以下、図面を参照して本発明に係る暗号化方法の実施の形態を説明する。

【0018】［暗号化方法に基づく暗号化を実行するファクシミリ装置の構成］まず、本発明に係る暗号化方法に基づく暗号化処理を実行するファクシミリ装置の構成を説明する。図1に示すように、本実施形態におけるファクシミリ装置10は、ファクシミリ装置10全体を制御するCPU12、CPU12を動作させるためのプログラムが格納されたメモリとしてのROM14、CPU12の動作に必要なデータを保存するメモリとしてのRAM16、オペレータからの入力の受け付け及びファクシミリ装置10の状態の表示を行う操作部18、CCD等を含んで構成され原稿を読み取りその読取データを2値化する画像読み取り部22、画像読み取り部22で2値化された画情報を圧縮符号化する符号器24、メモリを内蔵し、符号器24で符号化された画情報を前記メモリに書き込みCPU12と連携して前記画情報に対して暗号化処理を行うデータ処理部26、圧縮符号化された画情報を復号化する復号器28、画情報を記録用紙等に印字出力する画像記録部30、公衆回線34に接続され画情報を公衆回線34に送出するモデム回線制御部32、及び画像読み取り部22により読み取られた画情報やモデム回線制御部32により受信した画情報を一時的に記憶する画像記憶部20を含んで構成されており、これらはデータバス36を介して相互に接続されている。

【0019】［ファクシミリ装置の送受信動作］次に、上記ファクシミリ装置10の基本的な送受信動作を説明する。

【0020】まず、図2を用いて、送信動作を説明する。図2に示すステップ102で操作部18から送信指示を受けると、ステップ104へ進み、画像読み取り部22の所定位置に載置された原稿を画像読み取り部22によって読み取り、この読取で得られた画情報を符号器

24で符号化した後、該符号化した画情報を画像記憶部20に一旦蓄積する。

【0021】次のステップ106では画像記憶部20に蓄積された画情報を8バイトのブロック単位でデータ処理部26のメモリに転送し、DESで暗号化する。そして、暗号化された画情報はモデム回線制御部32に転送され、ステップ108でモデム回線制御部32によって前記暗号化された画情報を256バイト単位でITU-TのG3ファクシミリエラーコレクトモードで公衆回線34に送出する。このようにして、画情報は暗号化され目的のファクシミリ装置へ送信される。

【0022】以後、ステップ106、108を繰り返し、全ての画情報を暗号化し目的のファクシミリ装置へ送信する。但し、最終ブロックが8バイトに満たない場合は、後述するデータ埋め込み方法により該最終ブロックにデータを埋め込んだ後、暗号化を行う。

【0023】次に、図3を用いて、受信動作を説明する。図3に示すステップ202で外部のファクシミリ装置から、暗号化された画情報を受信すると、ステップ204で該受信した画情報をモデム回線制御部32によって2値データに変換した（即ち、復調した）後、データ処理部26のメモリに転送する。

【0024】次のステップ206では、データ処理部26のメモリ上で、送信時と同様に8バイト単位で前記復調された画情報をDESで復号化する。そして、次のステップ208で前記復号化された画情報を画像記憶部20へ格納する。以後、ステップ206、208を繰り返し、受信した全ての画情報を復号化し画像記憶部20へ格納する。

【0025】受信した全ての画情報の復号化・画像記憶部20への格納が完了すると、ステップ212へ進み、画像記憶部20から画情報を取り出して復号器28で伸張し、次のステップ214で画像記録部30によって前記伸張した画情報を記録用紙等に印字出力する。なお、上記画情報の伸張と印字出力において、最終ブロックについては、該最終ブロック内の画情報はページ終端符号RTCで終了しているので、該最終ブロック内の埋め込みデータ（後述するデータ埋め込み方法により埋め込まれたデータ）は無視される。

【0026】［本実施形態の作用］さて、これより本実施形態の作用として、本発明に係るデータ埋め込み処理を含む暗号化方法を、図5を用いて説明する。なお、RAM16の電源をオンした時にRAM16に記憶されていた所定データ量のデータ（例えば、RAM16の所定アドレスに記憶されていたデータ）をRAM16の初期データとしてRAM16に保存しておく。

【0027】図5のステップ152で、処理すべきデータを8バイトのブロック単位で（data[0]からdata[7]まで）読み込み、8バイトそろっていれば、ステップ166へ進み、DESにより暗号化する。

【0028】以後、8バイト単位でのDES暗号化を繰り返す。そして、処理すべきデータの終わりに近くなると、ステップ152で読み込んだデータが8バイトそろっていないケースが起こりうる。このように読み込んだデータが8バイトそろっていない場合はステップ156へ進み、RAM16に保存しておいたRAM16の初期データを変数a_0に代入する（初期データa_0を設定する）と共に、前記読み込んだデータのデータ数（バイト数）をカウンタiにセットする。

【0029】次のステップ158では初期データa_0を基に乗算合同法$16807 \times a_0 \pmod{2^{31}-1}$により発生させた擬似乱数を変数$a_1$に代入する（擬似乱数$a_1$を設定する）。なお、modは剰余演算、$2^{31}-1$は素数、16807はこの素数の原始根である。次のステップ160では擬似乱数a_1の下位1ビットをdata[i]とし、変数a_0に擬似乱数a_1を代入する（擬似乱数a_0を設定する）。

【0030】そして、変数iを1つインクリメントし（ステップ162）、変数iが8未満ならば、ステップ158へ戻り、擬似乱数a_0を基に乗算合同法$16807 \times a_0 \pmod{2^{31}-1}$により発生させた擬似乱数を再度変数$a_1$に代入する（新たな擬似乱数$a_1$を設定する）。そして、この擬似乱数$a_1$の下位1ビットをdata[i]とする（ステップ160）。

【0031】このようにして変数iが8以上になるまでdata[i]が順に生成されていく。ここで生成されるdata[i]は、読み込んだデータに対し8バイトに満たない部分を埋めるための埋め込みデータとなる。

【0032】例えば、図4に示すように、平文が3バイトであった場合は、RAM16を電源オンした時の初期状態を基に発生させた擬似乱数を残りの5バイトのデータ（data[3]～data[7]）として埋め込む。より具体的には、RAM16の初期状態を基に発生させた擬似乱数の下位1ビットをdata[3]に設定し、この擬似乱数を基に新たに発生させた擬似乱数の下位1ビットをdata[4]に設定する。このように擬似乱数を繰り返し発生させ、発生した擬似乱数の下位1ビットを埋め込みデータとして使用する。

【0033】そして、ステップ166において8バイトそろったデータ、即ちdata[0]からdata[7]までをDESで暗号化して、暗号化処理を終了する。

【0034】以上説明した暗号化処理によれば、最終ブロックの8バイトに満たない部分に盗聴者にとって予想困難なRAM16の初期データに基づく擬似乱数を埋め込むので、より解読困難な暗号化を行うことができる。

【0035】なお、図示は省略したが、受信側は8バイト単位でDESの復号を行う。後は、通常の符号データの復号を行いプリント出力する。画情報の最終データには埋め込みデータが付加されているが、画情報の終端はページ終端符号RTCによって認識できるので、埋め込みデータは無視され障害とはならない。

【0036】ところで、擬似乱数を発生させる基となるデータとしては、RAM16の初期データ以外にも、盗聴者にとって予想困難なデータであれば何でも用いることができる。例えば、前の暗号化処理における平文を用いても良く、同様の効果を得ることができる。

【0037】また、暗号化処理の待機中に連続して擬似乱数を発生させ、暗号化処理の開始時に発生した擬似乱数を、最終ブロックの8バイトに満たない部分に埋め込んでも良い。ここで、図6を用いて、暗号化処理の待機中に埋め込みデータを生成する処理を説明する。

【0038】RAM16の電源をオンした時にRAM16に記憶されていた所定データ量のデータ（例えば、RAM16の所定アドレスに記憶されていたデータ）を、RAM16の初期データとして読み取り変数a_0に設定する。この変数a_0を基に乗算合同法$a_1 = 16807 \times a_0 \pmod{2^{31}-1}$により擬似乱数$a_1$を発生させる。

【0039】暗号化処理が開始されるまでは、上記発生させた擬似乱数a_1を変数a_0に設定し、この変数a_0を基に上記乗算合同法により新たに擬似乱数a_1を発生させる。このようにして次々と擬似乱数は発生し続ける。

【0040】そして、暗号化処理が開始されれば、擬似乱数の発生を停止してこの時点の変数a_0の値を埋め込みデータの初期値として使用する。

【0041】この暗号化処理開始時点の変数a_0の値は、暗号化処理の待機状態に関する情報（例えば、待機の開始時刻や待機時間の長さ等）に相関するおそれもあるが、待機状態に関する情報は盗聴者にとって予想困難であるので、より解読困難な暗号化を行うことができる。さらに、暗号化処理開始時点の変数a_0の値を埋め込みデータの初期値として使用することで、より解読困難な暗号化を行うことができる。

【0042】なお、上記実施形態では、本発明に係る暗号化方法をファクシミリ装置に適用した例を示したが、本発明に係る暗号化方法は、ファクシミリ装置以外にも、データの送受信を行う機器全般に対して適用することができる。

【0043】

【発明の効果】本発明によれば、ブロック単位でのデータの暗号化に先立ち、所定のブロックサイズに満たないブロックについては、盗聴者にとって予想困難なデータを埋め込むので、より解読困難な暗号化を行うことができる。

【図面の簡単な説明】

【図1】発明の実施形態におけるファクシミリ装置の全体構成図である。

【図2】図1のファクシミリ装置における送信動作の処

理ルーチンを示す流れ図である。

【図３】図１のファクシミリ装置における受信動作の処理ルーチンを示す流れ図である。

【図４】発明の実施形態におけるデータ埋め込み処理の概要を示す図である。

【図５】図４のデータ埋め込み処理を含む暗号化処理の処理ルーチンを示す流れ図である。

【図６】暗号化処理の待機中に埋め込みデータを生成する処理の処理ルーチンを示す流れ図である。

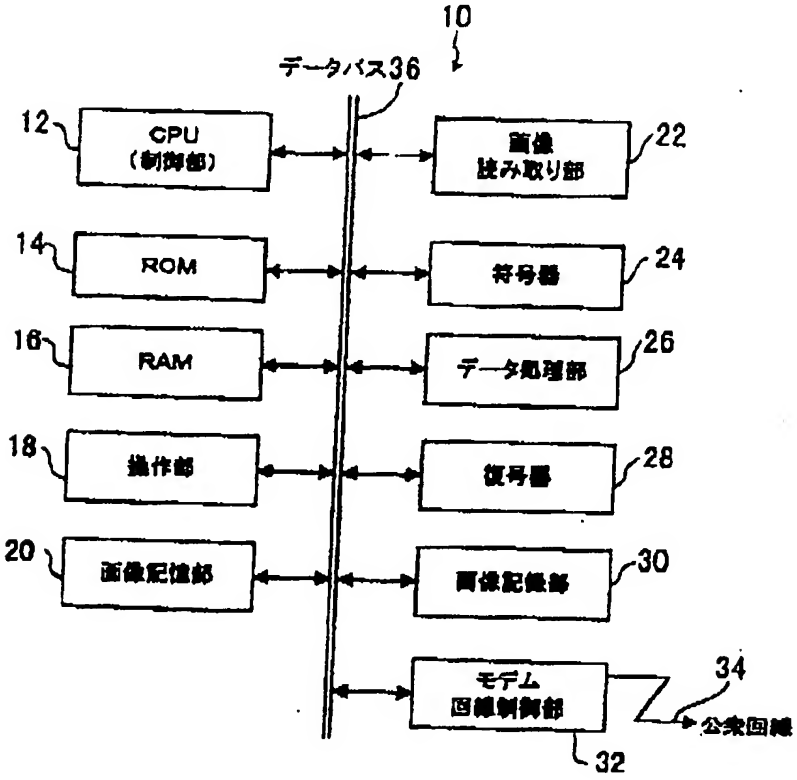
【符号の説明】

１０　ファクシミリ装置

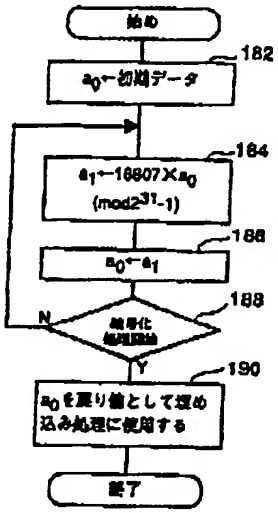
１２　ＣＰＵ

２６　データ処理部

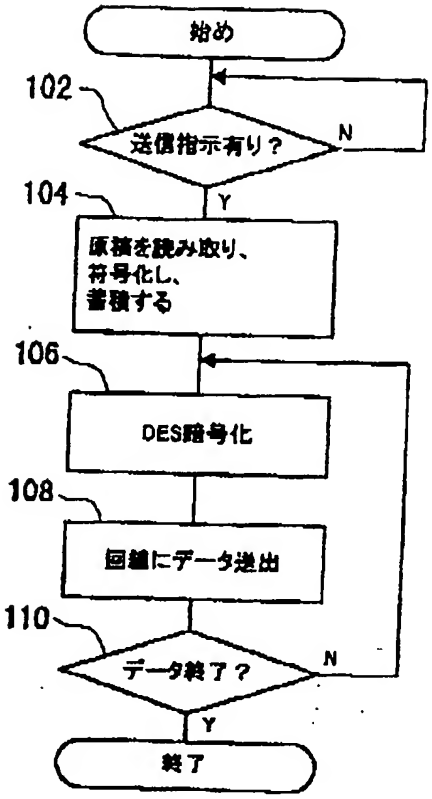
【図１】



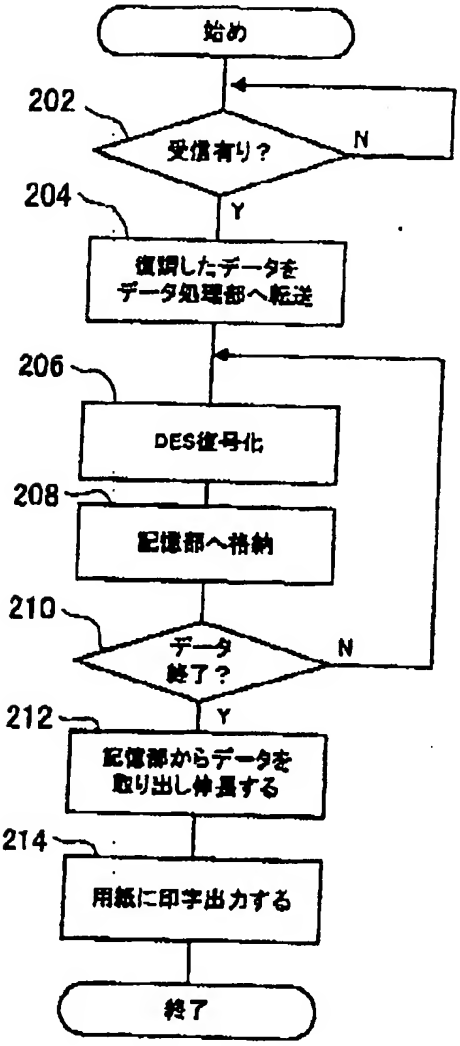
【図６】



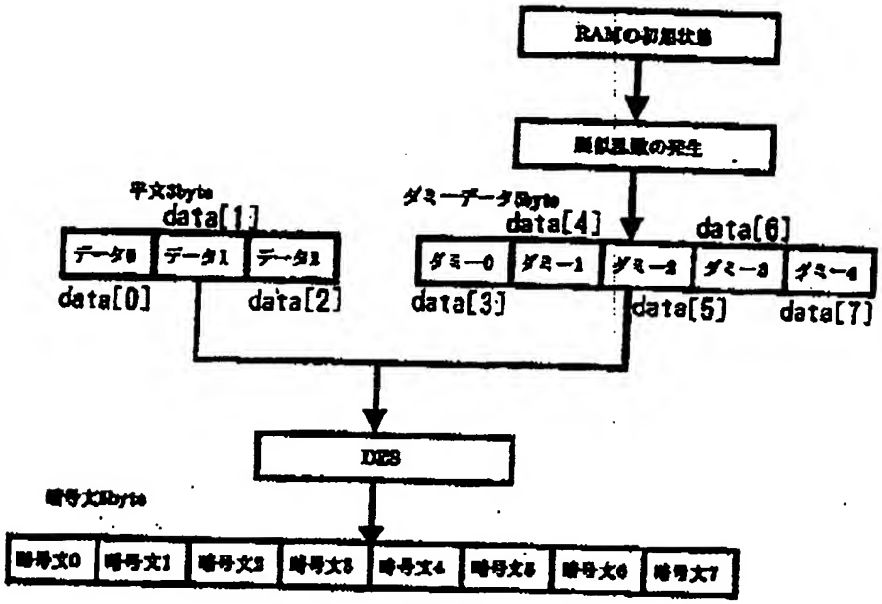
【図2】


始め
102
送信指示有り？
N
Y
104
原稿を読み取り、
符号化し、
蓄積する
106
DES暗号化
108
回線にデータ送出
110
データ終了？
N
Y
終了

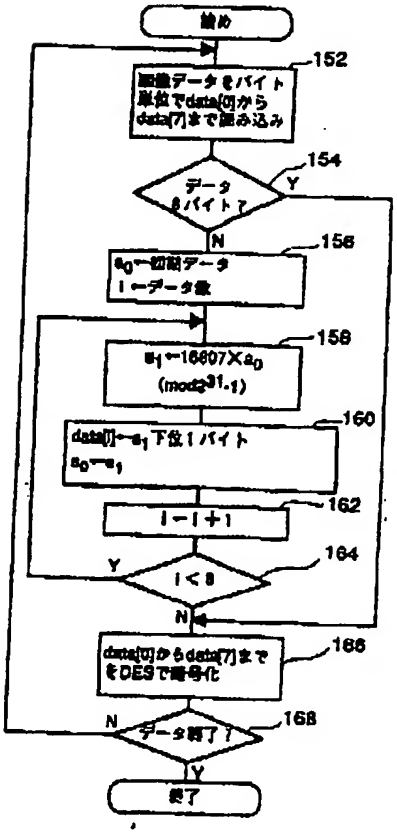
【図3】


始め
202
受信有り？
N
Y
204
復調したデータを
データ処理部へ転送
206
DES復号化
208
記憶部へ格納
210
データ
終了？
N
Y
212
記憶部からデータを
取り出し伸長する
214
用紙に印字出力する
終了

【図4】


RAMの初期状態
擬似乱数の発生
平文3byte
data[1]
データ0
データ1
データ2
data[0]
data[2]
ダミーデータ5byte
data[4]
data[6]
ダミー0
ダミー1
ダミー2
ダミー3
ダミー4
data[3]
data[5]
data[7]
DES
暗号文8byte
暗号文0
暗号文1
暗号文2
暗号文3
暗号文4
暗号文5
暗号文6
暗号文7

【図5】


始め
152
154
Y
N
156
158
160
162
164
Y
N
166
N
168
Y
終了